

Patent Application Docket #20661/457

WHAT IS CLAIMED IS:

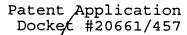
1	1.	An	electronic	module	used	for	secure	transactions
2	comp	comprising:				/		

- input/output circuitry for communicating to a data
 processing circuit;
- 5 math coprocessor circuitry electrically connected to 6 said input/output circuitry;
- microprocessor circuitry electrically connected to

 said input/output circuitry; and
- memory circuitry electrically connected to said
 microprocessor circuitry, said electronic module being
 programmable to provide secure, encrypted data transfers
 between said electronic module and said data processing
 circuit.
 - 2. The electronic module of claim 1, wherein said data processing circuit is another electronic module.
 - 1 3. The electronic module of claim 1, further comprising 2 a one-wire interface connected to said input/output 3 circuitry.

120

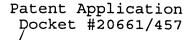




- 1 4. The electronic module of claim 1, wherein said
 2 memory circuitry is adapted to store a private
 3 encryption/decryption key for use during the encrypted
 4 data transfers between said electronic module and said
 5 data processing circuit.
- 1 5. The electronic module of claim 1, wherein said encrypted transactions are time stamped.
- 1 6. A system for communicating secure transactions,
 2 comprising:
- a first module comprising:
 - input/output circuitry;
- 5 random number dreating means for creating a
- 6 random number; and
- a first transaction group for requesting said random number creating means to create said random number and for providing said random number to said input\output
- 10 / circuitry; and
- a service provider equipment comprising:
- means for reading said random number from said
- input/output ci/cuitry of said first module;

Patent Application Docket #20661/457

- means for combining said random number with a
 first data and for encrypting the combination of said
 random number and said first data with a private key to
 produce a first certificate, whereby said input/output
 circuity of said first module is adapted to receive said
 first certificate.
 - 7. The system of claim 6, wherein said service provider equipment comprises a second module.
 - 8. The system of claim 6, wherein said first module further comprises an identifier for identifying said first module, and wherein said first transaction group provides said identifier to said input/output circuitry.
 - 9. The system of claim 8, wherein said means for reading is further for reading said identifier from said input/output circuitry of said first module.
 - 1 10. The system of claim 6, wherein said first module 2 further comprises a second transaction group.



and the properties of the second

- 1 11. The system of claim 6, wherein said module further
- 2 comprises a means for time stamping a complete
- 3 transaction.

4

7

8

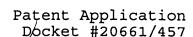
9

10

- 1 12. A method of communicating encrypted information
- between a module and a service provider equipment,
- 3 comprising the steps of:
 - a) creating a first random number in said module;
- b) passing said random number to said service provider equipment;
 - c) encrypting at least said random number with a private key in said service provider equipment thereby producing a certificate;
 - d) passing at least said certificate to said module;
- e) decrypting said certificate with a public key in said module;
- f) comparing said first random number with a number found in the decrypted first certificate of step e) to determine if the two numbers match.



- 1 13. The method of claim 12, wherein/step b) further
- 2 comprises the step of passing a module identifier to said
- 3 service provider equipment.
- 1 14. The method of claim 12/ wherein said service
- 2 provider equipment is another module.
- 1 15. The method of claim 12, wherein said method
- 2 incorporates a single wire bus.
- 1 16. The method of claim 15 wherein said single wire bus
- 2 is substantially a one-wire ous.
- 1 17. A method of / communicating encrypted information
- 2 between a module and a service provider equipment,
- 3 comprising the steps of:
- a) creating a first random number in said service
- 5 provider equipment;
- b) passing said random number to said module;
- 7 c) excrypting at least said random number with a
- 8 private key in said module thereby producing a first
- 9 certificate;



- d) passing at least said first certificate to said service provider equipment;
- e) decrypting said first certificate with a public key in said service provider equipment;
- f) comparing said first random number with a number
 found in the decrypted first certificate of step f) to
 determine if the two numbers match.
 - 1 18. The method of claim 17, wherein said service 2 provider equipment is another module.
 - 1 19. The method of claim 17, wherein said method incorporates a single wire bus.
 - 1 20. The method of claim 17, wherein said single wire bus 2 is substantially a one-wire bus.
 - 1 21. A method of decrypting encrypted data using a module, comprising the steps of:
 - receiving a first encrypted data and a second encrypted data;

9





5	decrypting said first encrypted data with a private
6	key stored in said module, whereby a first decryption key
7	is created;
8	providing said first decryption key to an electronic

system;

decrypting said second encrypted data with said first decryption key via said electronic system, whereby a useful information is created.

1 22. The method of claim 21, wherein said encrypted data 2 is an electronic mail message.

Add C1)